IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO

ORANGEBOY, INC., Plaintiff, v. PATRON POINT, INC., and DOES #1–5, Defendants.	Case No. 2:20-cv-4245 Judge James L. Graham Magistrate Judge Kimberly A. Jolson

PLAINTIFF ORANGEBOY, INC.'S MOTION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION AND FOR EXPEDITED DISCOVERY

Plaintiff OrangeBoy is the target of a coordinated effort by Patron Point, a direct competitor, to breach the security of OrangeBoy's computer systems, potentially exposing millions of third parties' privacy information, violating their privacy and irreparably harming OrangeBoy's business in the process. Patron Point has repeatedly tried to guess and reset passwords for user accounts belonging to OrangeBoy and to its clients. It has also used an "email subscription bomb" to sign up OrangeBoy users for thousands of email subscriptions, in an apparent effort to hide its password-guessing attempts in a flood of other messages. And it has employed a fake identity, claiming to be a potential client in an effort to obtain nonpublic information about OrangeBoy's technology.

Though these efforts have, so far, failed to breach OrangeBoy's security, they risk causing irreparable harm not only to OrangeBoy, but also to the clients and third parties who trust and rely on OrangeBoy to protect their private information.

OrangeBoy therefore asks this Court: (1) to enter a temporary restraining order and preliminary injunction prohibiting Patron Point from further action aimed at breaching OrangeBoy's security or obtaining unauthorized access to OrangeBoy's software platform; and (2) authorizing the parties to begin discovery immediately, on an expedited time frame, to ensure that OrangeBoy can gather supporting evidence from third parties, including internet service providers and social-media sites, before it is destroyed or deleted.

FACTUAL BACKGROUND

A. OrangeBoy and Patron Point.

Since 1996, OrangeBoy has provided consulting, analytics, and strategic-planning services to social-service and governmental entities, in particular public libraries, across the United States and Canada. (*See* Ex. A, Decl. of M. Clark Swanson II, ¶ 3.) Today, the company's services are centered around its web-based software platform, Savannah. Savannah uses advanced analytics and business intelligence reports to help OrangeBoy's library clients glean insights from their operations data. (*Id.* ¶ 4.) Savannah helps these clients act on those insights to improve their services offerings, build deeper relationships with their customers (typically, library cardholders), secure new customers, and increase philanthropic giving through targeted email communications and feedback mechanisms. (*Id.*) Over 125 public libraries in the United States and Canada currently use Savannah to gain meaningful insights about their operations and user bases, to communicate with their cardholders, and to gather feedback about their operations, programs, and interventions. (*Id.* ¶ 5.)

As a web-based platform, Savannah is not installed on users' computers like traditional software. (Ex. B, Decl. of Chris Kelbley, ¶ 3.) Rather, OrangeBoy partners with Microsoft to operate servers in the United States and Canada to securely host the Savannah software, back-end functionality, and client databases. (*Id.*) This allows users to access Savannah's functionality

and real-time analyses at any time, from any place, so long as they have access to the Internet and a standard web browser.

OrangeBoy takes the security of its software platform very seriously. (*Id.* ¶¶ 4–5.) Not only do OrangeBoy's clients trust OrangeBoy with data about their internal operations, but by using Savannah to engage with their own clients—library cardholders and other users of library services—these libraries also entrust OrangeBoy with certain information about those cardholders, such as names, email addresses, and other contact information. (*Id.* ¶ 4.) All told, OrangeBoy is responsible for securely storing information about more than 35 million library cardholders across North America. (*Id.*)

OrangeBoy's clients rightly expect OrangeBoy to keep this information safe and confidential. Because OrangeBoy's clients are typically governmental bodies, they are often subject to even more stringent data-security and privacy laws than private businesses would be. In any event, a security breach exposing this information to third parties could put these libraries' end-users at risk of identity theft and violate their expectations of privacy. Such a security breach would be a disaster for OrangeBoy, subjecting it to potentially enormous legal liabilities and causing irreparable harm to OrangeBoy's reputation. (*See* Ex. A, ¶¶ 7, 11.)

OrangeBoy therefore goes to great effort to ensure that its systems are secure and that its users' data remains safe and confidential. (*Id.* ¶ 7; Ex. B, ¶ 5.) It stores user data in independent, secure databases, anonymizing or pseudonymizing it wherever possible and ensuring that all transfers are made by secure means. (Ex. B, ¶ 5.) OrangeBoy then limits access to that data, and to Savannah more generally, by assigning user names and passwords to authorized users and requiring that each user provide appropriate credentials before they are allowed into the system. And it regularly monitors its systems for vulnerabilities and attacks. (*Id.*)

Patron Point is a competitor to OrangeBoy that offers marketing-automation software to libraries in Ohio and other states. (*See* Ex. A, ¶ 8.) Though its software does not include counterparts to all of the functionality provided by Savannah, the company claims to offer the same or similar services to Savannah at a lower price. (*See id.*)

B. OrangeBoy Observes Attempts to Breach Its Security and Links Those Attacks to Patron Point.

Earlier this year, Patron Point began ramping up its efforts to compete with OrangeBoy. Among other things, it had begun sending emails to OrangeBoy clients comparing its product favorably to Savannah, and it had bought advertisements on Google to show up when users searched for "OrangeBoy," "orange boy," and similar terms. (*See id.*, ¶ 8)

By midyear, however, Patron Point's competitive efforts had taken a more serious turn. On June 2, 2020, OrangeBoy detected an attempted attack on its system. (Ex. B, ¶ 6.) In particular, someone used Savannah's "Forgot Password" page to try to reset the Savannah passwords for several OrangeBoy email addresses, including that of the company's President, Sandy Swanson. (*Id.*) Around the same time, someone submitted fake information to a contact form on OrangeBoy's web site, seeking a demonstration of Savannah. (Ex. C, Decl. of Jaime Hirschfeld, ¶ 3–4.)

Though these efforts to gain access to Savannah did not succeed, OrangeBoy initiated an investigation into the activity. It traced the attacker's IP address[1] and determined two things: (1) the attack originated in or near Johnstone, Scotland, a town near Glasgow; and (2) the same IP

[1] Internet Protocol addresses, more commonly known as IP addresses, are unique numbers assigned to each device connected to a computer network, such as the Internet. They are used to identify computers on a network and to route communications to the correct recipients. Although sophisticated attackers often hide their true IP address by routing their actions through various third parties, in certain situations IP addresses can be traced back to particular persons or computers, or to certain parts of the world. (*See* Ex. B, ¶ 8.)

address had been used back in January when a user claiming the email address "scott.euan.downie@gmail.com" had tried (unsuccessfully) to log into Savannah. (Ex. B, ¶¶ 7–10.) These facts raised suspicions within OrangeBoy, as Patron Point had recently hired a Glasgow-based executive named Ian Downie as its Vice President of Growth. (*Id.* ¶ 11; see also Ex. D, Decl. of Joshua M. Feasel, ¶ 5.)

In late July, another attack on OrangeBoy's security drew closer scrutiny. (*See* Ex. B ¶¶ 12–17.) This attack was more sophisticated than June's attack had been. As with that first attack, this one involved attempts to guess and reset Savannah passwords. But this attack targeted OrangeBoy's ***clients***, not just its employees. (*See id.* ¶ 15.) Also as with the first attack, this one involved an attempt to gain information about OrangeBoy's technology. But whereas the first attack involved a fake name and non-working email address, this time the attacker created a fake email account to go along with his or her made-up identity. (*See id.* ¶ 16; Ex. C, ¶¶ 5–8.) This allowed the attacker to carry on a conversation with OrangeBoy's Sales Manager, which he or she did in the guise of a potential client: "Sara Morrison" at the "St. Paul Library." (*Id.*) In addition to these two prongs, the July attack included a new element: an "email subscription bomb" that resulted in OrangeBoy employees' email addresses being signed up for over 10,000 subscription lists. (*See* Ex. B, ¶¶ 13–14.) This element of the attack appeared to be aimed at taking OrangeBoy's email system offline, or at least degrading its service by slowing it down and overloading employees' inboxes with unimportant messages, making it more likely that an important message—such as an alert notifying OrangeBoy of efforts to guess and reset client passwords—would be overlooked. (*Id.* ¶¶ 14–15.)

Again, OrangeBoy was able to successfully fend off this attack, and again, it followed up by investigating the matter. This time, OrangeBoy's investigation found that all three attacks

originated with the same IP address and thus appeared to be part of a coordinated effort to breach OrangeBoy's security. (*See id.* ¶ 17.) The company also found that while "Sara Mortimer" from the "Saint Paul Library" did not appear to be a real person, her alter ego, "Beth Ryan"[2]—appeared to have a Twitter account. (*See* Ex. C, ¶¶ 7–8.) Indeed, OrangeBoy discovered what appear to be Twitter accounts for both "Beth Ryan" and the "St Paul Public Library." Interestingly, both of these accounts were created in May 2020; both accounts' only activity since they were created has been to retweet numerous marketing messages from Patron Point's corporate account; and neither account has shown any activity since the July attacks on OrangeBoy's system. (*Id.*; *see also* Ex. D, ¶¶ 3–4.)

Finally, OrangeBoy's investigation revealed further suspicious activity just before the July 29 attack began. Around that time, OrangeBoy's web site had been visited by IP addresses that traced back to Wilmslow, England, and to Johnstone, Scotland. (Ex. B, ¶ 18.) The LinkedIn account of Patron Point's Business Development Director, Nigel Wheeldon, lists the town of Wilmslow, England, as his location. (*See* Ex. D, ¶ 6.) And as noted above, Patron Point's Vice President of Growth, Ian Downie, appears to live near Johnstone, Scotland. (Ex. B ¶ 18.) This pattern of visitors alone struck OrangeBoy as abnormal, based on its past web site traffic and the fact that OrangeBoy does not provide services to any libraries in the United Kingdom and does not market Savannah in the United Kingdom. (*Id.*) Combined with the timing of these visits, however, and the information it had uncovered about "Sara Morrison" and "Scott Euan Downie," OrangeBoy found this information to be greatly concerning. (*Id.*)

[2] Whereas most of "Sara's" emails came from the email address "stpaullibrary@outlook.com," her final email to OrangeBoy's Sales Manager instead showed "Beth Ryan <beth.ryan100@gmail.com>" as the return address.

C. Patron Point Fails to Take Steps to Stop and Prevent Further Attacks.

On August 3, after having determined that Patron Point appears to be behind these attacks, OrangeBoy sent Patron Point a letter demanding prompt action. (*See* Ex. D, ¶ 7.) Despite its request—and its offer to help Patron Point with technical aspects of its investigation as necessary—Patron Point has failed to provide any substantive response to this letter in the more than two weeks since it was sent. (*See id.* ¶ 8.)

In light of the increased sophistication of the most recent round of attacks, as well as Patron Point's failure to respond substantively to OrangeBoy's correspondence, OrangeBoy filed the present lawsuit in an effort to ensure the continued security of its systems and its clients' data.

LAW AND ARGUMENT

OrangeBoy asks this Court for two forms of relief. First, it asks that this Court enter a temporary restraining order and preliminary injunction barring Patron Point from further attempts to breach OrangeBoy's security or to obtain unauthorized access to OrangeBoy's software platform. This relief is necessary and appropriate to ensure that OrangeBoy does not suffer irreparable harm during the litigation of this suit.

Second, OrangeBoy asks the Court to authorize immediate and expedited discovery. Such an order is appropriate not just to ensure that the parties can prepare their cases for a preliminary injunction hearing, but also to ensure that OrangeBoy can gather supporting evidence from internet service providers, social-media sites, and other third parties before it is destroyed or deleted as a matter of course.

A. OrangeBoy Is Entitled to Temporary and Preliminary Injunctive Relief.

In determining whether to enter a temporary restraining order or injunctive relief, the courts consider four factors: (1) whether the movant has a strong likelihood of success on the

merits; (2) whether the movant would suffer irreparable injury without an injunction; (3) whether issuing an injunction would substantially harm others; and (4) whether an injunction would serve the public interest. *See McPherson v. Michigan High School Athletic Ass'n, Inc.*, 119 F.3d 453, 459 (6th Cir. 1997). These considerations "are factors to be balanced, not prerequisites that must be met." *Jones v. City of Monroe*, 341 F.3d 474, 476 (6th Cir. 2003).

As is carefully explained below, here each of the four factors favors injunctive relief.

1. OrangeBoy is likely to succeed on the merits.

First, OrangeBoy is likely to succeed on the merits of its claim. The facts discussed above show that OrangeBoy already has ample evidence tying Patron Point to the attacks on OrangeBoy's system. Discovery from Patron Point and third parties is likely to corroborate and supplement that evidence, providing a basis for identifying the Doe defendants and further linking this activity to Patron Point.

Nor can Patron Point argue that it has a legal right to engage in this conduct. For one thing, guessing passwords to gain access to a computer system is a clear breach of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. The CFAA bars persons from intentionally accessing a "protected computer"—that is, a computer used in interstate commerce, *id.* § 1030(e)(2)—either without authorization or by exceeding the person's authorized access, and obtaining information thereby. *Id.* § 1030(a)(2). It separately bars persons from causing damage and loss by intentionally accessing a protected computer. *Id.* § 1030(a)(5)(C). Conspiracies and attempts to violate the CFAA are themselves violations of the CFAA. *Id.* § 1030(b).

Here, OrangeBoy's servers are "protected computers" because their use to provide access to Savannah across the United States and Canada constitutes interstate commerce. Patron Point does not have authority to use Savannah, yet it attempted to access that software, and thus the information that it stores and makes use of, by trying to guess the passwords of users who did

have that authority. Its attempts harmed OrangeBoy—and risked causing irreparable harm, not only to OrangeBoy, but also to its clients and to the individual library cardholders whose data OrangeBoy is tasked with protecting. These efforts were thus a paradigmatic violation of the CFAA. *See, e.g.*, *United States v. Batti*, 631 F.3d 371, 373 (6th Cir. 2011); *United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991) (upholding conviction under CFAA where "there was … evidence that the worm was designed to gain access to computers at which he had no account by guessing their passwords").

Though the CFAA is found in Title 18 of the U.S. Code, it creates both criminal and civil liability for violations of its terms, and OrangeBoy has a right to bring a civil cause of action in response to this violation. The CFAA expressly allows "[a]ny person who suffers damage or loss by reason of a violation" of the statute to bring a civil suit for "compensatory damages and injunctive relief or other equitable relief," so long as the violation meets one of several additional requirements. *Id.* § 1030(g). In particular, an attempted violation meets the requirements for civil suit where the attempted violation, if completed, would have caused a loss of at least $5,000 in value. *Id.* § 1030(c)(4)(A)(i)(I). Here, Patron Point's attack risked a core principle underlying OrangeBoy's business: its customers' trust that their data would remain secure. A breach of OrangeBoy's data security would cause incalculable harm to the company's reputation, in addition to legal liabilities totaling hundreds of thousands, if not millions, of dollars. (*See* Ex. A, ¶ 7.)

Moreover, because Patron Point's conduct violated the criminal laws, OrangeBoy has a civil cause of action under Ohio Rev. Code 2307.60. *See id.* ("Anyone injured in person or property by a criminal act has … a civil action unless specifically excepted by law…."); *see also Buddenberg v. Weisdack*, __ Ohio St.3d __, 2020-Ohio-3832, ¶ 14 (holding that Revised Code

2307.60 "does not require" an underlying criminal conviction, but only a criminal act). In addition to the CFAA violation discussed above, Patron Point's conduct violated a number of other criminal statutes, including but not limited to Ohio Revised Code 2913.04 (prohibiting persons from "attempt[ing] to gain access to … any computer [or] computer system … without the consent of, or beyond the scope of the express or implied consent of, the owner of the computer [or] computer system"), Ohio Revised Code 2913.05 (prohibiting the use of telecommunications data to execute or further a scheme to defraud), and 18 U.S.C. § 1832 (prohibiting the attempted theft of trade secrets).

Finally, Patron Point's use of unlawful and deceptive means, including an email subscription bomb and a false identity, to obtain nonpublic information about—not to mention unauthorized access to—OrangeBoy's software platform makes it liable under Ohio's common law of unfair competition. *See, e.g.*, *Water Management, Inc. v. Stayanchi*, 15 Ohio St.3d 83, 472 N.E.2d 715 (1984) ("The concept of unfair competition may also extend to unfair commercial practices such as malicious litigation, circulation of false rumors, or publication of statements, all designed to harm the business of another.").

Under each of these theories, OrangeBoy is substantially likely to succeed on the merits. For that reason, the first injunctive-relief factor weighs strongly in OrangeBoy's favor.

2. An Injunction Is Necessary to Prevent Irreparable Harm.

The second factor also supports OrangeBoy's motion, because without injunctive relief, OrangeBoy risks suffering irreparable harm. An injury is irreparable when it cannot be fully compensated by money damages, or when the proper measure of damages would be difficult to calculation. *See Overstreet v. Lexington-Fayette Urban Cty. Gov.*, 305 F.3d 566, 578 (6th Cir. 2002); *United States v. Miami Univ.*, 294 F.3d 797, 819 (6th Cir. 2002).

Just so here. Though Patron Point's first two attacks have both failed to breach OrangeBoy's security, the second attack proved to be substantially more sophisticated than the first. A third attack may well prove even more sophisticated; in any event, even an unsophisticated attempt at guessing a user's password may succeed if given enough tries. Moreover, while the first attack targeted OrangeBoy's accounts only, the second attack began to target the accounts of OrangeBoy's clients. A data breach exposing the data of OrangeBoy's clients, however, would be disastrous, not only to OrangeBoy's reputation, but also to the third parties whose data would be exposed.

The harm from such a breach would include not only the potential legal liability to OrangeBoy, but also the indirect effects of a breach on the company's goodwill, its potential clients' trust in the company, and their resulting willingness to go into business with it. OrangeBoy's business is heavily dependent on its customers' confidence that OrangeBoy will be able to protect their data and hold it in confidence. The full measure of this harm would thus be difficult if not impossible to calculate. *See Basicomputer Corp. v. Scott*, 973 F.2d 507, 512 (6th Cir. 1992) ("The loss of customer goodwill often amounts to irreparable injury because the damages flowing from such losses are difficult to compute."). Indeed, it is likely that ***no*** damages award could fully make up for the harm caused by a security breach, particularly given that a direct competitor is involved in the breach. *See* Singapore Ministry of Health v. Farrera-Brochez, No. 5:19-051-DCR (E.D. Ky. Nov. 25, 2019) (holding that consumer loss of confidence in plaintiff constitutes irreparable harm); *cf. Basicomputer*, 973 F.2d at 512 ("[T]he loss of fair competition that results from the breach of a non-competition covenant is likely to irreparably harm an employer.").

OrangeBoy cannot simply wait around for a successful attack before taking legal action. Without an injunction from this Court, its clients' data remains at risk of a third, successful attack. This is not a situation likely to make OrangeBoy's customers feel confident in the continued security of their data. Thus, an injunction is required to maintain the status quo and ensure that OrangeBoy is not irreparably harmed during the pendency of this action.

3. Injunction Will Not Cause Substantial Harm to Patron Point or Third Parties.

For the same reasons, not only will injunctive relief not cause substantial harm to others, but rather is necessary to ***avoid*** such harm. OrangeBoy's clients, not to mention those clients' cardholders, rely on OrangeBoy to keep their data confidential and secure. A data breach exposing that data would significantly, and irreparably, harm those third parties.

Nor will an injunction cause Patron Point significant harm. Patron Point holds no legitimate interest in seeking unauthorized access to a competitor's computer systems, or even in using a fake name and institutional affiliation to seek nonpublic information about competitors. It thus has little ground to complain about the requested injunction.

4. Granting an Injunction Will Serve the Public Interest.

Finally, the public interest supports an injunction here. Maintaining the confidentiality of OrangeBoy's clients' data—and that of their individual cardholders—is in the public interest. There is no counterbalancing principle that could find a public interest in allowing corporations to use deceptive and fraudulent conduct to interfere with their competitors' businesses.

B. The Court Should Authorize Immediate, Expedited Discovery to Ensure that Relevant Evidence Is Not Inadvertently Destroyed.

Under Rule 26(d)(1), parties may not seek discovery "from any source" before their Rule-26(f) conference, unless authorized by rule, stipulation, or court order. Relatedly, the courts have authority to expedite party discovery by shortening the ordinary timing requirements for

good cause. *See* Fed. R. Civ. P. 33(b)(2), 34(b)(2)(A), 36(a)(3). OrangeBoy asks the Court to authorize the parties to begin seeking discovery immediately—and to order that the parties respond to each other's discovery requests on an expedited basis. Such an order will not only help the parties prepare for a preliminary injunction hearing. More importantly, it will help prevent the inadvertent destruction of relevant evidence by third parties.

Because of the distributed nature of the Internet, third parties are often the best sources of information that can be used to identify the people using a web-based service or visiting a web site. Here, for instance, OrangeBoy has been able to use its attackers' IP addresses to ascertain some information about them. But the Internet Service Providers to whom those IP addresses were assigned would almost certainly be able to give more information about those persons—through activity logs or even subscriber information. Similarly, Twitter, Inc. knows more about the persons behind the "St. Paul Library" and "Beth Ryan" accounts than OrangeBoy can glean from reviewing and cross-referencing their posts.

But if OrangeBoy is not able to seek this information promptly, these sources of information may be lost. Internet service providers' activity logs are likely regularly deleted under standard document-retention policies. A 90-day retention period, for instance, would mean that information regarding the June 2 attack will be destroyed in early September. The same goes for information regarding the late-July attack, if subject to a 30-day retention period. Either way, the delay involved in waiting for a Rule-26(f) conference may be enough to allow this evidence to be lost. That risk counsels in favor of allowing immediate discovery.

CONCLUSION

For the reasons set forth herein, (1) OrangeBoy, Inc.'s motion for a temporary restraining order and preliminary injunction should be granted, and (2) this Court should authorize the parties to begin seeking discovery immediately and on an expedited time frame.

Dated: August 20, 2020

/s/ Joshua M. Feasel
Joshua M. Feasel (0090291)
Feasel PLLC
P.O. Box 6842
Detroit, MI 48202
734.726.0016
313.217.3509 (f)
jmfeasel@feaselpllc.com

Attorney for Plaintiff OrangeBoy, Inc.

CERTIFICATION OF COUNSEL

Pursuant to Federal Rule of Civil Procedure 65(b)(1)(B), the undersigned hereby certifies that on August 20, 2020, he provided a copy of the Complaint, with exhibit, and advance copies of this Motion and all supporting documents to legal counsel for Defendant Patron Point, Inc. by email.

/s/ Joshua M. Feasel
Attorney for Plaintiff OrangeBoy, Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on August 20, 2020, a true and accurate copy of the foregoing document was served by email upon the following:

Sterling Weiser
Vesha Law Firm, LLC
38 South High Street
Dublin, OH 43017
sterling@veshalaw.com

Attorney for Defendant Patron Point, Inc.

/s/ Joshua M. Feasel
Attorney for Plaintiff OrangeBoy, Inc.